

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-312078

(43)公開日 平成11年(1999)11月9日

(51)Int.Cl.⁶

G 0 6 F 7/58

1/04

識別記号

3 0 1

F I

G 0 6 F 7/58

1/04

A

3 0 1 A

審査請求 未請求 請求項の数1 O L (全 4 頁)

(21)出願番号

特願平10-120757

(22)出願日

平成10年(1998)4月30日

(71)出願人 000116024

ローム株式会社

京都府京都市右京区西院溝崎町21番地

(72)発明者 田切 宏和

京都市右京区西院溝崎町21番地 ローム株式会社内

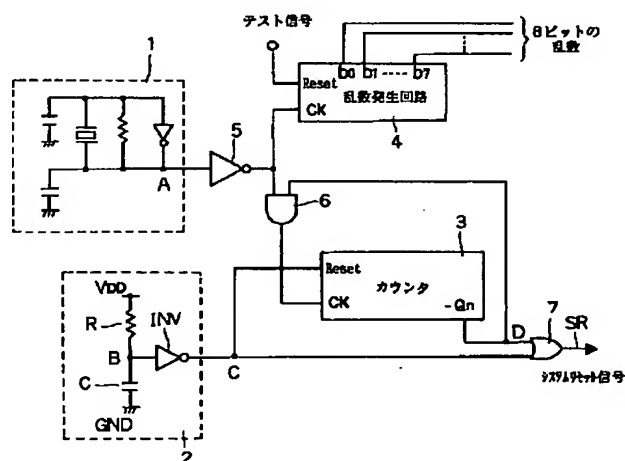
(74)代理人 弁理士 佐野 静夫

(54)【発明の名称】 乱数発生回路を有する半導体装置

(57)【要約】

【課題】 カウンタ構成の乱数発生回路を有する半導体装置であって、電源投入直後に乱数を使用する回路によって読み出される乱数の値が常に同一となることがないようにした半導体装置を提供する。

【解決手段】 入力クロックに同期して所定系列の乱数を出力する乱数発生回路4を有する半導体装置において、乱数発生回路4については、電源投入後、初期化することなく、さらに、クロックが不安定な状態で、動作を開始させるようにする。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 半導体集積回路を同期動作させるためのクロック信号を発生する発振回路と、前記半導体集積回路の論理状態を確定させるためのリセット信号を発生する初期化回路と、前記クロック信号に同期して所定系列の乱数を発生する乱数発生回路とを有する半導体装置であって、

前記乱数発生回路は、前記リセット信号で初期化されることがないとともに、前記発振回路の動作が不安定な状態でも前記クロック信号が入力されるように構成されていることを特徴とする半導体装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、入力クロックに同期して所定系列の乱数を出力する乱数発生回路を有する半導体装置に関するものである。

【0002】

【従来の技術】 通常、システムにおいては、電源投入時には、安定動作を確保するため、システム全体を初期化するとともに、クロックの発振が安定するまでリセットをかける（動作させない）ようになっており、乱数を出力する乱数発生回路を有するシステムの場合も同様であった。

【0003】

【発明が解決しようとする課題】 ここで、乱数を出力する乱数発生回路がカウンタ構成（入力クロックに同期して所定系列の乱数を出力する構成）である場合、リセット解除後の同じタイミングで得られる乱数の値は必ず同じである。

【0004】 また、通常、乱数を使用する回路では、リセット解除後、入力クロックのカウント数によって乱数を読み出すようになっており、常に同じタイミングで乱数を読み出すことになる。

【0005】 以上より、乱数発生回路を有する従来の乱数発生システムでは、乱数発生回路がカウンタ構成である場合、乱数を使用する回路によって電源投入直後に読み出される乱数は常に同じ値となってしまう。

【0006】 そこで、本発明は、カウンタ構成の乱数発生回路を有する半導体装置であって、電源投入直後に乱数を使用する回路によって読み出される乱数の値が常に同一となることがないようにした半導体装置を提供することを目的とする。

【0007】

【課題を解決するための手段】 上記の目的を達成するため、本発明では、半導体集積回路を同期動作させるためのクロック信号を発生する発振回路と、前記半導体集積回路の論理状態を確定させるためのリセット信号を発生する初期化回路と、前記クロック信号に同期して所定系列の乱数を発生する乱数発生回路とを有する半導体装置であって、前記乱数発生回路は、前記リセット信号で初

期化されることがないとともに、前記発振回路の動作が不安定な状態でも前記クロック信号が入力されるようにしている。

【0008】 以上の構成により、電源投入後、乱数発生回路は出力する乱数の初期値を与えられることなく動作を開始し、また、動作を開始してから一定時間が経過するまでに入力されるクロックの数は不定となり、システム全体（乱数発生回路を除く）のリセット解除後の同じタイミングであっても、乱数発生回路から出力される乱数は常に同じ値となることはない。

【0009】

【発明の実施の形態】 以下に、本発明の実施形態を図面を参照しながら説明する。図1は本発明の一実施形態である半導体装置の構成を示す図である。同図において、1はクリスタルの発振回路、2はパワーオンリセット回路、3はカウンタ、4はカウンタ構成の乱数発生回路、5はインバータ回路、6はAND回路、7はOR回路である。

【0010】 発振回路1の発振波はインバータ回路5を介して乱数発生回路4のクロック端子CK及びAND回路6に入力される。AND回路6のもう一方の入力にはNビットのバイナリカウンタとして構成されたカウンタ3の出力端子-Qnが接続されており、AND回路6の出力はカウンタ3のクロック端子CKに接続されている。

【0011】 パワーオンリセット回路2の出力は、カウンタ3のリセット端子Resetに接続されているとともに、OR回路7の入力に接続されている。OR回路7のもう一方の入力にはカウンタ3の出力端子-Qnが接続されている。

【0012】 そして、OR回路7の出力（以下、「システムリセット信号SR」と呼ぶ）は、乱数発生回路4が出力する乱数を使用する回路（不図示）に入力されており、この乱数を使用する回路は、システム全体のリセットが解除された後（システムリセット信号SRがハイレベルからローレベルになった後）、入力されるクロックを所定数カウントすると、乱数発生回路4が出力する乱数を読み出すようになっており、常に同じタイミングで乱数が読み出されることになる。

【0013】 パワーオンリセット回路2は、電源電圧V_{DD}とグラウンドGND間に直列接続された抵抗RとコンデンサCとの接続点がインバータINVの入力に接続されており、その出力（インバータINVの出力側）は、電源投入直後はハイレベルとなるが、コンデンサCと抵抗Rとによって決まる所定時間t₀が経過するとローレベルに切り換わる。

【0014】 カウンタ3は、リセット状態（リセット端子Resetに入力される信号がハイレベルである状態）では、出力端子-Qnからの出力をハイレベルとするが、リセット解除後（リセット端子Resetに入力

3

される信号がハイレベルからローレベルに切り換わった後)、クロック端子CKに入力されるクロックの立ち上がりをもとに所定回数カウントすると、出力端子Qnからの出力をローレベルに切り換える。

【0015】尚、カウンタ3がクロック端子CKから入力するクロックの立ち上がりをもとにカウントする回数は、カウンタ3の出力端子Qnからの出力が、電源投入後、発振回路1の発振波が安定した後に、ローレベルに切り換わるように設定されている。

【0016】乱数発生回路4は、例えば、図3に示すようなカウンタ構成であり、この例では、8つのフリップフロップFF1～FF8が縦続接続され、これらの縦続接続間のうち、フリップフロップFF2とフリップフロップFF3との間、フリップフロップFF3とフリップフロップFF4との間、フリップフロップFF5とフリップフロップFF6との間に、それぞれEXOR回路G1、G2、G3が設けられ、最終段の出力が初段のフリップフロップFF1の入力、及び、各EXOR回路G1～G3に帰還されている。これにより、各段の入力からなる8ビットには、クロック端子CKに入力されるクロックに同期して所定系列の乱数が現れることになる。

【0017】尚、乱数発生回路4はリセット端子Resetを有しており、このリセット端子Resetに入力される信号によってリセットがかかり、乱数として出力する初期値が与えられるが、このリセット端子はシステム内部ではどこにも接続されておらず、正常に動作しているか否かを判定することなどを目的として、テスト時にのみ、外部からリセット端子に信号を入力し、乱数発生回路4に外部からリセットをかけることができるようになっている。

【0018】以上より、電源投入後の、発振回路1の発振波A、パワーオンリセット回路2のコンデンサCと抵抗Rとの接続点Bの電圧、パワーオンリセット回路2の出力C、カウンタ3の出力D、及び、システムリセット信号SRのタイミングチャートは図2に示すようになり、電源投入後、時間 $t_0 + t_1$ が経過すると、すなわち、発振回路1の発振が安定した後に、システム全体のリセットが解除され、その後、さらに時間 t_2 が経過すると、乱数が読み出されることになる。尚、 t_0 はパワーオンリセット回路1のコンデンサCと抵抗Rとで決まる時間、 t_1 はカウンタ3がクロックの立ち上がりをもとに所定回数カウントするまでに要する時間、 t_2 は乱数を使用する回路がクロックを所定回数カウントするまでに要する時間である。

【0019】したがって、システム全体のリセットが解除された後、常に同じタイミングで乱数が読み出されることになるが、本実施形態では、乱数発生回路4については、電源投入後、初期化することなく、さらに、発振回路1の発振波が不安定な状態で、動作を開始させることになるので、初期値を与えられることなく動作を開始

4

し、また、動作を開始してから一定時間が経過するまでに入力されるクロックの数は不定となり、これにより、電源投入直後に読み出される乱数の値は常に同一となることはない。

【0020】尚、カウンタ構成の乱数発生回路については、トランジスタの能力のアンバランスなどにより、リセットをかけなくても、電源投入時に出力する乱数の値が同一になる場合があるが、このような場合でも、本実施形態では、さらに、入力クロックが不安定な状態から動作させるようにしているので、電源投入後、一定時間が経過するまでに入力されるクロックの数は不定であり、乱数を使用する回路によって読み出される乱数の値は常に同一となることはない。

【0021】さらに、本実施形態では、コンデンサCと抵抗Rのばらつきによって、電源投入後、パワーオンリセット回路2の出力がハイレベルからローレベルに変化するまでの時間、ひいては、システムリセットが解除されるまでの時間がばらつくので、乱数を使用する回路によって電源投入後に読み出される乱数の値はシステム毎に異なるものとなる。

【0022】尚、本発明は、上記実施形態に限定されるものではなく、例えば、発振回路1、パワーオンリセット回路2、カウンタ3、及び、乱数発生回路4については、様々な構成を取り得る。また、発振回路1及びパワーオンリセット回路2については、IC内部であってもIC外部であってもどちらでも構わない。

【0023】

【発明の効果】以上説明したように、乱数発生回路を有する本発明の半導体装置によれば、電源投入後、乱数発生回路は初期値を与えられることなく動作を開始し、また、動作を開始してから一定時間が経過するまでに入力されるクロックの数は不定となるので、システム全体（乱数発生回路を除く）のリセットが解除された後、同じタイミングで乱数が読み出されたとしても、その値が常に同一となることはなくなる。

【図面の簡単な説明】

【図1】 本発明の一実施形態である半導体装置の構成を示す図である。

【図2】 各信号のタイミングチャートを示す図である。

【図3】 カウンタ構成の乱数発生回路を示す図である。

【符号の説明】

- 1 発振回路
- 2 パワーオンリセット回路
- 3 カウンタ
- 4 乱数発生回路
- 5 インバータ回路
- 6 AND回路
- 7 OR回路

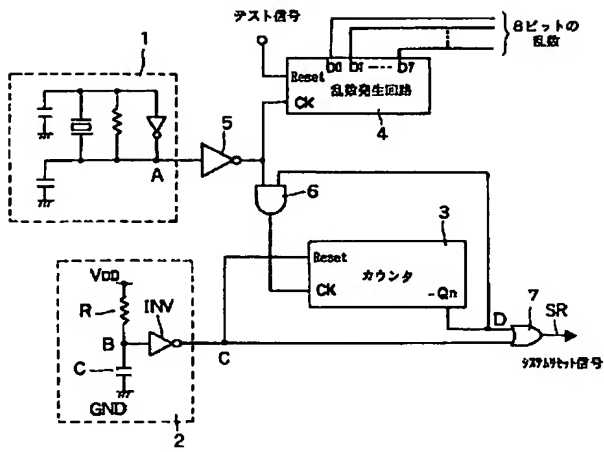
(4)

特開平 11-312078

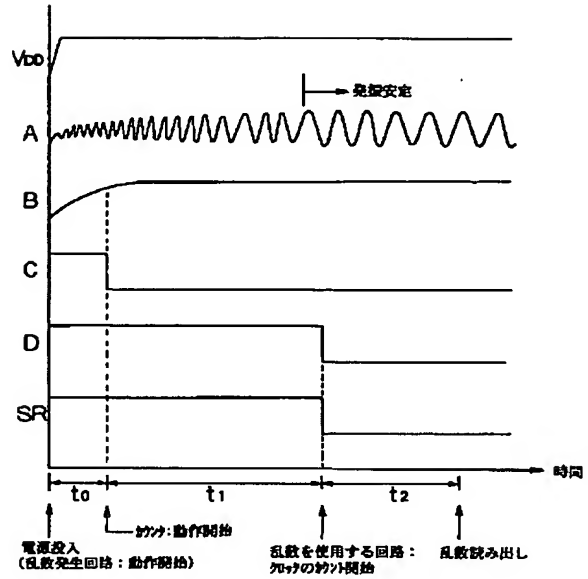
5
FF1~FF8 フリップフロップ

6
G1~G3 EXOR回路

【図1】



【図2】



【図3】

